准备和应对拒绝服务攻击

初版日期：2011年9月
最后更新：2025年3月

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

简介

本出版物由澳大利亚信号局（Australian Signals Directorate，简称ASD）会同新西兰国家网络安全中心（New Zealand's National Cyber Security Centre，简称NCSC-NZ）、Akamai科技有限公司和Cloudflare有限公司共同编制，旨在应对本地区拒绝服务（DoS）攻击日益增多的趋势。本出版物依据当代威胁技术，为组织提供符合最佳规范的缓解措施指南，以准备和应对DoS攻击。

我们建议您结合ASD出版的*《物联网设备》（Internet of Things devices）*及*《保护您的Wi-Fi和路由器》（Secure your Wi-Fi and router）*等出版物来阅读本公告议。这些出版物可帮助个人避免在无意中助长DoS攻击，而这种攻击可能会对他人造成影响。

DoS攻击是一类网络攻击，旨在破坏或降低网站、电子邮件和域名系统（DNS）服务等在线服务的功能，从而导致合法用户无法访问。通常，这是通过向某一在线服务发送海量数据、连接或请求，从而使其不堪重负并降低其功能来实现的。

DoS攻击通常需要大量网络流量才能奏效。这种攻击正变得越来越普遍，部分原因是容易受到入侵的物联网（IoT）设备的数量增加。由于物联网设备制造商往往优先考虑用户体验而非网络安全，一些连接到互联网的普通家用物品——例如智能电视、电热水壶、吸尘器和安全系统——也可能成为易受攻击的设备。这些设备通常会被恶意行为者远程入侵，组成一个设备“僵尸网络”（'botnet'）来生成这种网络流量，从而导致家庭和组织无意中助长促成DoS攻击发生的基础设施。

最近的活动表明，一旦恶意行为者入侵了大量物联网设备，他们可能会将这些基础设施出租或出售给网络犯罪分子和黑客活动分子，而这些人越来越倾向于针对其选定的目标发起DoS攻击。在大多数情况下，DoS攻击的目的是为了造成组织的生产效率下降和经济损失，或为了引起公众对某项事业的关注。ASD在其发布的题为*《与中华人民共和国有关联的行为者入侵路由器和物联网设备进行僵尸网络行动》（People's Republic of China-linked actors compromise routers and IoT devices for botnet operations）*公告中描述了此类活动的一个案例。

随着我们的经济进一步数字化，而且越来越多安全性较差的物联网设备接入互联网，DoS攻击可能会继续增加。

为了干扰或降级组织的在线服务，恶意行为者会采用多种手段，包括：

- 将大量不必要的网络流量导向在线服务，试图消耗其所有可用的网络带宽
- 将特定设计的网络流量导向在线服务，试图消耗其计算机处理资源
- 使用多台计算机、物联网设备或其他连接互联网的设备，从多个方向、更大规模地将网络流量导向在线服务，这是一种常见的DoS攻击类型，称为分布式DoS（DDoS）攻击
- 劫持组织的注册域名或DNS服务器，试图将合法用户引导到错误的在线服务，从而无法访问原本的在线服务。

组织无法避免成为DoS攻击的目标，但可以采取多种措施来做好防范，并可能减轻影响。最好的策略是在DoS攻击发生之前就做好防范。如果没有准备，在DoS攻击期间作出应对的难度就会很大，而且效果更差。

尽管组织主要关注的焦点在于保护自己免受DoS攻击，但也应该采取措施防止其在线服务和连接互联网的设备被恶意行为者滥用来攻击他人。

做好应对DoS攻击的准备

我们整个地区DoS攻击数量不断增加，在此背景下，贵组织在实施任何应对DoS攻击的防范措施之前，应首先评估自己的业务需求，以确定在遭遇DoS攻击期间，是否必须保持各项在线服务持续运行，还是可以接受暂时的服务中断。

如果贵组织希望增强抵御DoS攻击的能力，就应在DoS攻击发生之前，在适当且可行的情况下主动实施以下措施。

- 如果贵组织正在使用内容分发网络（CDN），则应在适当且可行的情况下实施以下附加措施。
  - 考虑使用具备保护源Web服务器免受各种应用程序和网络层攻击功能的CDN——某些CDN可能含有这些功能，而这些功能是位于网络边缘的Web应用程序防火墙的一部分。
  - 避免不必要地公开披露您的源Web服务器的互联网协议（IP）地址，并确保任何公开暴露的部分都受到保护，免受DoS攻击。
  - 避免为您的源Web服务器使用恶意行为者可以预测的IP地址，如与您的在线服务公开披露的IP地址位于同一网络子网中的IP地址。
  - 使用网络访问控制机制（如防火墙），确保只有CDN和贵组织授权的管理网络能够访问您的源Web服务器。
  - 如果您需要对源Web服务器进行更高级别的保护，考虑在源Web服务器和CDN供应商之间使用具备复原力和多样性的网络连接，其中可包括专用网络连接。
  - 配置CDN、源Web服务器和客户端HTTP标头，以优化所执行的缓存量。
  - 如果您需要更高级别的可用性，建议对源Web服务器进行分区，以便将较低风险IP地址的请求与较高风险IP地址的请求分开进行处理。
- 确定您的在线服务的合法用户可接受的功能和服务质量标准、应如何维护该功能、哪些功能在DoS攻击期间可以暂停。
- 采购并使用基于云的DoS攻击缓解服务。
- 考虑通过以下方式缩小贵组织的受攻击面：
  - 将基础在线服务（如DNS）外包给能够抵御DoS攻击的信誉良好的服务供应商
  - 将关键在线服务（如电子邮件）与更有可能成为攻击目标的其他在线服务（例如网站）进行分区管理
  - 确保DoS攻击缓解服务仅允许与在线服务所用网络端口相关的网络流量通过。

- 与您的服务供应商详细沟通其DoS攻击预防和缓解策略，具体而言包括以下方面：
  - 是否具备抵御来自世界各地的DoS攻击的能力
  - 是否有成功应对DoS攻击和经过授权的综合性DoS攻击测试的记录
  - 是否能够自动缓解大多数类型的DoS攻击而无需人工干预（如手动分析网络流量）
  - 服务计费方法，例如其费用是固定的还是根据所使用的网络流量和计算机处理资源而变化，以及是否可以设置计费上限
  - 在遭受DoS攻击期间通知您或关闭其在线服务的阈值
  - 在DoS攻击期间可以采取的预先批准的措施
  - 与上游供应商之间的DoS攻击防护协作机制。
- 实施各项措施来检测DoS攻击，如对系统可用性、网络流量、计算机处理资源使用情况和相关成本的实时监控和警报。
- 为贵网站准备一个对处理和带宽要求最低的静态版本，以便在DoS攻击期间保持服务的持续可用性。
- 采购并使用高韧性在线服务，此类服务具有充足的带宽、充裕的计算机处理资源、地域分散的托管位置和用于清除异常网络流量的基于云的流量清理机制——这通常包括使用信誉良好的CDN来缓存静态网站内容，并保护您的源Web服务器，使其免受恶意网络流量的侵害。
- 采取措施保护贵组织的域名安全，这些措施包括使用域名注册商锁定、确认域名注册联系方式和其他详细信息正确无误、遵循ASD发布的*《域名所有者的域名系统安全》（Domain Name System security for domain owners）*中的附加指南。
- 确保持有服务供应商的最新联系方式，并向其提供贵组织的联系方式，确保所有联系人均能按照贵组织的要求（如每周7天、每天24小时）保持联系。
- 通过可信赖的通信渠道，为贵组织设立带外通信联系方式，并将此联系方式提供给您的服务供应商，以便在正常通信渠道出现故障时，依然能够保持联系。
- 制定、实施和维护一套网络安全事件响应计划，该计划应涵盖针对每一项在线服务的各种类型的DoS攻击，每年至少演练一次。
- 设计应用程序，保护常被滥用的功能，这些功能会消耗更多的计算机处理资源或产生额外的经济成本（如发送短信）。
  - 实施保护机制，如速率限制和人机验证。
  - 执行DoS攻击测试，包括针对应用程序功能中的非正常逻辑路径进行测试。
  - 执行更广泛的负载测试，以识别和修复DoS向量。

应对DoS攻击

如果贵组织尚未对DoS攻击做好防范，您可以尝试在遭受DoS攻击时实施上述部分措施，但效果可能有限，且执行过程可能耗费时间，从而削弱贵组织的应对能力。

在遭受DoS攻击期间，贵组织应在适当且可行的情况下实施以下措施。

- 启动网络安全事件响应计划。
- 询问您的服务供应商是否能够立即采取应对措施——如果事先未沟通相关的应对能力，您可能会发现其无法或不愿应对，或者会额外收取费用。
- 禁用使当前DoS攻击有效的非重要功能，或从在线服务中删除使当前攻击有效的非重要内容，如部署没有搜索功能、动态内容或大文件的网站版本。
- 与您的客户和服务供应商（包括您的DoS攻击缓解服务供应商）保持沟通，并持续监控在线服务的可用性。

- 如果您的源Web服务器正受到直接攻击，可考虑更改其IP地址，并避免在没有采取保护措施的情况下公开披露新的IP地址。
- 向有关各方（包括ASD和NCSC-NZ）报告DoS攻击事件，具体联系方式详见本出版物的“联系方式”章节。

避免助长DoS攻击

贵组织应实施以下措施，以避免无意中助长可能影响他人的DoS攻击。

- 避免将不需要的、配置不安全或维护不足的服务、物联网设备和其他可联网的设备暴露在互联网上。
- 妥善配置、维护和监控暴露在互联网上的服务、物联网设备和其他可联网的设备。
  - 有关小型企业的更多指南，请参阅ASD发布的*《物联网设备》（Internet of Things devices）*和*《保护您的Wi-Fi和路由器安全》（Secure your Wi-Fi and router）*。

如果贵组织正在运营在线服务，您应该实施以下附加措施。

- 优先查阅美国网络安全和基础设施安全局（Cybersecurity and Infrastructure Security Agency，简称CISA）发布的*《基于UDP的放大攻击》（UDP-Based Amplification Attacks）公告*中所罗列的协议。
- 持续监控新出现的放大攻击向量，保护您的在线服务免受其侵害。
- 配置入站和出站网络访问控制，仅允许授权的在线服务和组织的访问。
- 如非必要，对易于放大攻击的在线服务，应禁止匿名公共访问。
- 如果无法或不适宜实施阻止或访问控制，应考虑实施速率限制机制来降低滥用的影响。

更多信息

ASD的*《信息安全手册》（Information security manual）*是一个网络安全框架，各组织可以应用该框架来保护其系统和数据免受网络威胁。*《网络安全事件的缓解策略》（Strategies to mitigate cybersecurity incidents）*中的建议以及《八项基本成熟度模型》（Essential Eight）对这一框架进行了补充。

*《新西兰信息安全手册》（New Zealand Information Security Manual）*是新西兰政府关于信息保障和信息系统安全的手册。这是一本从业者手册，旨在满足机构信息安全主管以及为机构提供服务的厂商、承包商和顾问的需求。

有关各种DoS攻击类型的更多信息，请参阅由CISA出版的*《DDoS快速指南》（DDoS Quick Guide）*和*《了解和应对分布式拒绝服务攻击》（Understanding and Responding to Distributed Denial-Of-Service Attacks）*。

联系方式

在澳大利亚，如果您对本指南有任何问题，请写信给ASD或致电1300 CYBER1 (1300 292 371)。

在新西兰，如果您要报告网络安全事件，请发送电子邮件至incidents@ncsc.govt.nz或访问新西兰国家网络安全中心（NCSC-NZ）的“报告事件”（Report an incident）网页。

如需了解更多信息或报告网络安全事件，请联系我们：

cyber.gov.au | 1300 CYBER1 (1300 292 371)

该号码仅可在澳大利亚境内拨打。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre